Department of Homeland Security Daily Open Source Infrastructure Report for 07 December 2007

Current Nationwide

ELEVATED
Significant Risk of Terrorist Attacks

For info click here

- USA Today reported on a new Government Accountability Office report, which states that the nation faces "a high risk of a catastrophic runway collision," and efforts to improve the problem have stumbled due to lackluster federal leadership, technology glitches, and poor data collection. The GAO also called on the FAA to address fatigue among its air-traffic controllers. (See item **9**)
- According to the International Herald Tribune, the U.S. Agriculture Department recently announced its twentieth recall of ground beef this year because of contamination with E. coli. The recall count is one shy of a record set in 2000 and matched in 2002, and is surprising because in the two previous years recalls were in single digits. The cause for the jump remains unclear, but a number of theories have been offered. (See item **11**)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − [http://www.esisac.com]

1. *December 6, Star Bulletin* – (Hawaii) **Power failures linger after storm.** Power failures triggered by a storm that reached Oahu late Tuesday continued along the Waianae Coast and through scattered communities Thursday morning as Hawaiian Electric Co. (HECO) worked into the night Wednesday to replace dozens of damaged poles and fix downed lines. Wind gusts as strong as 70 mph that rushed through the island cut electricity to at least 45,000 HECO customers, about 15 percent of the company's 293,000 Oahu clients, said a company spokesman.

Source: http://starbulletin.com/2007/12/06/news/story01.html

2. *December 5, Platts* – (Utah) **Murray reopens Utah mine after brief shutdown.** Murray Energy's Utah subsidiary reopened the West Ridge mine in Carbon County on Tuesday night after halting production for about 48 hours because of a sudden increase in the ash content of the coal, a company official said Wednesday. "The mine resumed full production [Tuesday night] as we were able to secure an outlet for the high-ash coal," said the vice president of business development and external affairs at Murray Energy.
Source: http://www.platts.com/Coal/News/6639183.xml?sub=Coal&p=Coal/News&?undefined&undefined

[Return to top]

Chemical Industry Sector

3. *December 6, Associated Press* – (Kentucky) **Nerve agent leak in Kentucky could hasten chemical weapons destruction.** One gallon of liquid nerve agent seeped through a canister this summer at a chemical weapons stockpile in Kentucky - the largest leak ever detected there and one that has Army officials moving to destroy some of the weapons far ahead of schedule. Blue Grass Army Depot officials discovered the leak of liquid sarin August 27 during weekly inspections of the igloos that house the chemical weapons in Richmond set to be neutralized by 2017 to comply with an international treaty. In response, a citizens advisory board will meet Friday in Richmond to hear a proposal the Army is considering that would dramatically accelerate the destruction of the leaky container and two similar ones at the depot, said the panel's co-chair.
Source: http://www.kentucky.com/471/story/251432.html

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

4. *December 6, Greenville News* – (South Carolina) **Oconee Nuclear has follow-up safety plan.** Oconee Nuclear Station in South Carolina has addressed safety concerns and has a follow-up plan to correct any similar issues elsewhere, plant officials told the Nuclear Regulatory Commission on Wednesday. Regulators with the commission met with Duke Energy officials in a public meeting at the nuclear station to discuss results of a recent supplemental inspection related to three issues that were found by workers at the nuclear station and reported to the commission in 2005 and 2006. The problems involved a breach in a standby shutdown facility wall, debris in a sump pump line, and an outage at the Keowee hydro facility.
Source: http://greenvilleonline.com/apps/pbcs.dll/article?AID=/20071206/NEWS01/712060329

5. *December 4, WGAL 8 York* – (Pennsylvania) **Former supervisor talks about nuclear**

plant security. Monday, the Nuclear Regulatory Commission revealed the findings of its investigation into sleeping guards at the Peach Bottom Nuclear Plant in Pennsylvania. Investigators said they uncovered cases where employees were encouraged to hide what was going on and some did so out of fear for their jobs. Now a former security supervisor says the problem is even bigger than the government may think. The former supervisor oversaw the security force and its training, and he described a "culture of fear" amongst the plant's security personnel. He said not only did guards fear for their jobs, it went up through the ranks. On Monday, the NRC confirmed it found some of what he was talking about during its investigation. "There were incidents where individuals actually said they were discouraged and we had occasions where supervisors actually discouraged individuals from bringing inattentive issues forward," the NRC's senior security inspector, said at Monday's meeting.
Source: http://www.wgal.com/news/14774065/detail.html

[Return to top]

Defense Industrial Base Sector

6. *December 6, Los Angeles Business* – (National) **Northrop to compete for $3.8B Air Force contract.** Northrop Grumman Corporation said Thursday that it will be competing for a nine-year contract from the U.S. Air Force worth up to $3.8 billion. The contract would cover logistics support for the KC-10 aircraft and global logistics, maintenance, and repair support for the aerial refueling system for the KDC-10 aircraft. Both planes are used for refueling and transport. The Boeing Co. will also be competing for the project. The companies are also competing for the Air Force's KC-X contract, which is potentially worth $40 billion.
Source:
http://www.bizjournals.com/losangeles/stories/2007/12/03/daily31.html?ana=from_rss

7. *December 4, Associated Press* – (National) **Lockheed Martin wins $51.3M Army deal.** Lockheed Martin Corporation said it received a $51.3 million contract from the U.S. Army to supply additional helicopter-mounted missile launchers and launcher electronic assemblies for domestic and international forces. The contract also includes multiple spares, engineering services, and depot support. Deliveries are scheduled to run through the third quarter of 2011.
Source: http://biz.yahoo.com/ap/071204/lockheed_martin_army_contract.html?.v=1

[Return to top]

Banking and Finance Sector

8. *December 6, KBIA 91.3* – (Missouri) **Phishing scam targets Mid-Missourians.** The attorney general's office is warning Mid-Missourians of a new phishing scam involving Jefferson City based Central Bank. Callers to Missouri's Consumer Protection Hotline say they are receiving automated phone calls directing them to a specific website that asks for personal information. In other instances, live callers ask for the information. An official said the scam is similar to one right now in southwest Missouri involving

Empire Bank, and added they have seen this kind of scam throughout the state before.
Source:
http://publicbroadcasting.net/kbia/news.newsmain?action=article&ARTICLE_ID=1193910&sectionID=1

[Return to top]

Transportation Sector

9. *December 5, USA Today*– (National) **GAO: U.S. airports face risk of 'catastrophic runway collision.'** The nation faces "a high risk of a catastrophic runway collision" and efforts to improve the problem have stumbled due to lackluster federal leadership, technology glitches, and poor data collection, according to a Government Accountability Office (GAO) report released Wednesday. The Federal Aviation Administration (FAA) has failed to update its runway safety plan in five years, cut funding to its runway safety office, and did not appoint a permanent head of the office for two years, said the report. While the most serious incidents reported on the nation's runways fell to 24 in fiscal 2007 from 31 the previous year, the overall total of so-called "runway incursions" has gone up. The total number of incursions hit 370 in fiscal 2007, the highest since 2001. Furthermore, "the absence of coordination and national leadership impedes further progress on runway safety because no single office is taking charge of assessing the causes of runway safety problems and taking the steps needed to address those problems," the report added. The GAO also called on the FAA to address fatigue among its air-traffic controllers.
Source: http://www.usatoday.com/travel/news/2007-12-05-runway-collisions_N.htm

10. *December 5, FLIR Systems, Inc.* – (National) **FLIR Systems announces $2 million awards to boost airport security.** FLIR Systems, Inc. announced that it has received multiple awards totaling $2 million during 2007 to supply thermal security cameras to airports around the U.S. FLIR's thermal and multi-sensor security cameras were selected for installation at major airports throughout the country, including Dallas-Fort Worth, Cincinnati, Indianapolis, and the New York area's four major airports -- Kennedy, LaGuardia, Newark and Teterboro. The installations are part of the Department of Homeland Security's domestic airport Perimeter Intrusion Detection initiative. FLIR's performance features enable them to see intruders at night without expensive and intrusive lighting infrastructure making them flexible and effective airport security tools.
Source: http://money.cnn.com/news/newsfeeds/articles/marketwire/0336475.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.

[Return to top]

Agriculture and Food Sector

11. *December 6, International Herald Tribune* – (National) **Beef industry struggles in fight against E. coli.** The U.S. beef industry says it spends upward of $350 million a year to keep harmful pathogens out of the meat it sells to the public, but even as expenditures keep rising, the industry appears to be losing ground. Late last month, the U.S. Agriculture Department announced its twentieth recall of ground beef this year because of contamination with a toxic strain of E. coli. That is only one recall shy of a record set in 2000 and matched in 2002. What makes this year's spate of recalls so surprising is that it comes after several years in which the number of recalls dropped sharply – to eight in 2006 and five in 2005. No one knows for sure what is causing the jump in recalls, though theories range from the cyclical nature of pathogens to changes in cattle-feeding practices caused by the popularity of ethanol. USDA officials say that the only way to prevent E. coli contamination is to irradiate meat, a practice the federal government deems safe. Meat companies, however, have been hesitant to use irradiation because of fears that it would make meat more expensive, change the taste and color, and provoke consumer opposition.
    Source: http://www.iht.com/articles/2007/12/06/business/meat.php?page=1

12. *December 6, San Francisco Chronicle* – (California) **Recall of Metromint water sold online.** Soma Beverage Co., a small San Francisco company, issued a voluntary recall Wednesday of its mint-flavored water because of possible contamination, saying it found an isolated case of Bacillus cereus contamination in a water sample bottled a year ago at a Southern California plant. Bacillus cereus contamination can cause food poisoning, with symptoms including nausea and diarrhea. The Metromint water was sold in 16.9-ounce plastic bottles in peppermint, spearmint, orangemint, and lemonmint flavors. The recall involves water with a "Best before 2006/12/21" date printed on the shoulder of the bottle.
    Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/12/06/BAC3TP6RN.DTL

[Return to top]

Water Sector

13. *December 6, Atlanta Journal-Constitution* – (Georgia) **Drought presents chance for cleanup at Allatoona.** In Georgia, Lake Allatoona's retreating waters have exposed more than 50 years of sediment that contains contaminants such as phosphorus, a nutrient that feeds algae. In turn, algae make it more difficult and expensive to clean the water for drinking. State officials are in preliminary talks with the U.S. Army Corps of Engineers to use the current Southeast drought as an opportunity to dig out potentially millions of cubic yards of this sediment and cart it away before the lake levels rise and cover it all up again. This could restore some of the reservoir's original capacity to hold more water for the next drought. Removing 100,000 cubic yards of soil from the shores, for example, would cost $1 million and would increase capacity to provide only six additional hours of water service to the area, according to the Cobb County-Marietta Water Authority. Removing the sediment and phosphorus from the reservoir could make

it cheaper for the utility to clean the water for drinking. Because of the increased algae in the lake, the utility was forced to spend roughly $500,000 extra on chemicals to clean the water this year, said the general manager of the Cobb County-Marietta Water Authority. The Lake Allatoona Preservation Authority must now submit a plan and an environmental assessment to get approval from the Army Corps, which owns the reservoir. That plan must show how much debris would be removed and where it would be stored.
Source:
http://www.ajc.com/metro/content/metro/cobb/stories/2007/12/05/allatoona_1206.html

14. *December 5, KNSD 7/39 San Diego* – (California) **Fouled water prompts warnings.** An unknown amount of partially treated sewage spilled into the ocean from the Point Loma Wastewater Treatment Plant Wednesday, prompting county health officials to issue a warning. The leak was discovered during a morning maintenance inspection. As a result, officials have posted pollution warning signs along a section of Sunset Cliffs Park and a tide-pool area at Cabrillo National Monument. To the south, officials issued warnings about ocean water contaminated with sewage from the Tijuana Slough National Wildlife Refuge north to include the Imperial Beach shoreline. The areas will remain off limits until follow-up tests show that they are safe again for recreational uses, officials said.
Source: http://www.nbcsandiego.com/news/14784291/detail.html

[Return to top]

Public Health and Healthcare Sector

15. *December 6, McClatchy Newspapers* – (National; International) **Pharmaceutical drugs made in China may mean trouble for U.S.** China's booming pharmaceutical industry has doubled exports to the United States in the past five years, undercutting competitors and making American consumers reliant on the safety of Chinese factories and captive to any disruptions in China-U.S. commerce. While mainly a trade issue, industry experts in Europe and the U.S. say that national security concerns are edging into the debate. For example, if a major anthrax attack were to occur in the U.S., pharmaceutical companies that make the two antibiotics most suitable for treatment, Cipro, and doxycycline, would have no choice but to rely on China or India for key ingredients once American stockpiles were exhausted. Those ingredients are no longer made in the West. The U.S. would be forced to rely on a Chinese industry that is awash in problems and corruption. Recently, a kickback scandal charged China's State Food and Drug Administration and its chief with approving bogus drugs, including a counterfeit antibiotic that left 13 people dead. China executed the agency chief in July.
Source: http://www.kansascity.com/105/story/391581.html

16. *December 5, Associated Press* – (National) **35 percent of toys contain lead, report says.** A coalition of U.S. environmental health groups tested more than 1,200 children's products for lead, cadmium, arsenic and other toxic chemicals. Lead was found in 35 percent of the products tested. About 17 percent of the products had lead levels above the federal recall standard for lead paint and only 20 percent of toys and children's

products had no trace of lead or harmful chemicals. The Consumer Action Guide to Toxic Chemicals in Toys, which is available to the public at http://www.healthytoys.org, shows how the commonly purchased children's products rank in terms of containing lead, cadmium, arsenic and other harmful chemicals.
Source: http://www.msnbc.msn.com/id/22103641/

Government Facilities Sector

17. *December 6, Union-Tribune* – (California) **Fake bomb in UCSD lab leads to FBI investigation.** An anonymous caller to the University of California, San Diego campus threatened to detonate a bomb inside a biomedical lab building, an FBI spokesman said Wednesday. After the call was made, a campus employee found a suspicious device made to look like a bomb, on the first floor of the Leichtag Family Foundation Biomedical Research Building. The FBI Joint Terrorism Task Force responded because the target of the threat is a research facility, the spokesman said. Animal research is conducted at the medical school, but the official declined to say whether the bomb threat was related to that type of research. Authorities evacuated the building and seven others affiliated with the medical school, a campus spokeswoman said. No other devices were found.
Source: http://www.signonsandiego.com/news/metro/20071206-9999-1m6pubsafe.html

18. *December 6, Pantagraph Publishing* – (Illinois) **Possible chemical reaction causes smoke at ISU.** Fumes from a barrel used for disposing chemicals used in Illinois State University's science laboratories led fire officials to don chemical suits and try to find the cause of the leak Wednesday afternoon. Firefighters were called about noon to the east side of the ISU Science Laboratory Building after someone spotted fumes coming from a 55-gallon waste barrel next to the building. No buildings in the area were evacuated and no one was injured, but firefighters from Bloomington's hazardous materials team emptied the container because of a possible risk to those close to the barrel, he said. The barrel is used to store smaller containers of waste after chemicals are used in science projects.
Source:
http://pantagraph.com/articles/2007/12/06/news/doc4756f52fc7b03652252814.txt

19. *December 6, Florida Today* – (Florida) **Justice Center reopens after bomb threat.** Brevard County sheriff's deputies responded to a bomb threat Thursday morning at the Harry T. Moore Justice Center in Viera, Florida. A man called 911 from a pay phone in Palm Bay saying there was a bomb on each floor of the courthouse, dispatchers said. The caller said he was targeting the circuit judge because she gave either his friend or brother 30 years, sheriff's deputies reported. The courthouse was evacuated, but no device was found.
Source:
http://www.floridatoday.com/apps/pbcs.dll/article?AID=/20071206/BREAKINGNEWS/71206006/1086

20. *December 5, Minnesota* Daily – (Minnesota) **Willey Hall evacuated for bomb threat.** The University of Minnesota received a bomb threat for Willey Hall Wednesday morning, according to a University alert text message received at 11:30 a.m. Classes were temporarily canceled and police conducted a search of the building. The search found no suspicious items, according to a University emergency text message, and afternoon classes resumed at 12:45 p.m. This is the third bomb threat on campus this semester.
Source: http://www.mndaily.com/articles/2007/12/05/72164881

21. *December 5, Sacramento Bee* – (California) **Woodland police blow up suspicious package.** Police officers in Woodland, California, blew up a suspicious package left in front of City Hall Wednesday afternoon. City Hall was evacuated for nearly two hours and Court Street between First and College streets was blocked off before a bomb squad robot destroyed the package, police said. No one appeared to be injured.
Source: http://www.sacbee.com/101/story/546118.html

22. *December 5, WESH 2 Orlando* – (Florida) **Arrest made in connection with school bomb threats.** Another arrest was made on Tuesday after a threat at Central Middle School in west Melbourne, Florida. A note was scrawled on a torn-out sheet of notebook paper, police said. Police were called and they evacuated the school for two hours. This was the ninth bomb threat this year at CMS and the seventh arrest. Even though students have watched classmates go to jail, police said it has not stopped the threats. Police are now demanding stronger action from courts to punish the offenders. Police said the 15-year-old boy confessed when interviewed, and then confessed to another bomb threat in October.
Source: http://www.wesh.com/news/14779005/detail.html

[Return to top]

Emergency Services Sector

23. *December 5, Associated Press* – (Northwest) **Officials: ham radio operators are storm's 'unsung heroes.'** When parts of Oregon were overwhelmed by wind and water during the recent storm, vital communication often was lacking, with trees down and across phone lines and cell coverage limited. Even the state police had difficulty in reaching some of their own troops. But ham radio worked. In fact, amateur radio operators were heralded by state emergency officials as heroes. Ham radio is more than just a hobby to some. It can set up networks for government and emergency officials to communicate when other communication services fail. "One of the problems in this is always communication," said Oregon's governor Tuesday. "I'm going to tell you who the heroes were from the very beginning of this...the ham radio operators. These people just came in and actually provided a tremendous communication link to us." A network of at least 60 volunteer amateur radio operators working along the coast and inland helped from keep crucial systems such as 911 calls, American Red Cross and hospital services connected. They relayed information about patient care and relayed lists of supplies needed in areas cut off by water. In addition to getting an FCC license to operate, certain groups of operators are cleared by the federal government to work as

emergency responders. The Oregon Office of Emergency Management said the radio operators were tireless in their efforts to keep the systems connected. It was ham radio that kept New York City agencies in touch with each other after their command center was destroyed on 9-11, according to the National Association for Amateur Radio. When hurricanes like Katrina hit, amateur radio helped provide life-and-death communication services when everything else failed.
Source: http://www.kptv.com/weatheralert/14776224/detail.html

24. *December 6, vnunet.com* – (National) **VoIP must connect to emergency services.** VoIP services that allow users to make calls to normal national phone numbers must also have the ability to connect to emergency numbers 999 and 112 from 8 September 2008. Ofcom wants to ensure that users who have switched to VoIP services from traditional landline or cellular phone companies can still access the relevant people in emergencies. The watchdog expressed concern that consumers needing to locate an ordinary landline or mobile phone in an emergency might face a delay of seconds or even minutes in getting through. "As new voice services develop and become more mainstream, regulation must evolve too," said the entity's chief executive. "Consumers must be confident that, if they can make calls to ordinary national numbers using their VoIP service, they will be able to call 999 or 112 in an emergency." Ofcom found that 78 per cent of VoIP users who cannot currently call 999 or 112 either believed that an emergency call was possible, or did not know whether or not this was the case. The ruling attempts to protect consumers amid increasing use of VoIP services and the trend to look and feel more like traditional fixed and mobile phone services. Some commentators have voiced concerns over a reliance on VoIP technology, following the Skype outage earlier this year.
Source: http://www.vnunet.com/vnunet/news/2205253/ofcom-voip-connect-emergency

[Return to top]

Information Technology

25. *December 6, BetaNews* – (International) **Canada's passport application system has security hole.** An Ontario man discovered last week that the Web site meant to allow Canadians to apply for passports was allowing access to information on other applicants. By changing a single character in the URL while filling out the application, he was able to pull up data on another applicant. He told The Globe and Mail that doing so was effortless, and the site did nothing to prevent him from viewing the data. This leak provides enough data to essentially commit identity theft, it includes names, addresses, dates of birth, social insurance (Canada's social security) numbers, phone numbers, and drivers license data. The extent of the data breach is not known as Passport Canada did not give details on how many applicants may be sitting in queue on the site at any given time. It is also not clear if the data continues to sit on the site, accessible by its unique URL, after an application has been approved. In any case, access to the online application was disabled after the man informed the agency of the problem, and Passport Canada said it had the problem fixed by last Friday. However, a test on Monday by Globe and Mail reporters indicated that the hole still existed, and they were able to access further private data. This was despite Passport Canada's assurances that the

application was indeed secure. Unlike many parts of the US, there is no law requiring government agencies or companies to disclose security breaches to consumers. Supporters of such legislation in Canada are using the incident as an example of why laws in this area are needed.
Source:
http://www.betanews.com/article/Canadas_passport_application_system_has_security_hole/1196966059

26. *December 06, Computerworld* – (National) **Duke Law School applicants warned of possible ID theft.** About 1,400 Duke Law School applicants and two current students are being warned about identity theft concerns after hackers broke into the law school's Web site, where their Social Security numbers were stored in a connected database. In an announcement yesterday, the school said those affected are being notified of the incident via e-mail and letters sent by mail. "We have no evidence that the intruders actually downloaded or acquired any of this information," wrote the law school's associate dean of admissions in the email Tuesday. "Nonetheless, we know they had the opportunity and the tools to do so," he conceded. The incident was discovered by school officials last week, and the site -- which collects information from would-be applicants who want information about Duke from the admissions office -- was taken offline, according to the school. Those potentially affected by the breach had provided their Social Security numbers online. While investigating the breach, school officials said they also discovered that a second database could also have been accessed by hackers, potentially affecting another 1,900 people who filed online admissions applications to the law school. That database didn't included Social Security numbers, but held home addresses, phone numbers, e-mail addresses and passwords created as part of the application process, according to the school. Those 1,900 applicants were also notified of the breach on Tuesday via e-mail and were advised to change their account passwords. A spokeswoman for Duke said an investigation into the incidents is continuing. So far, she said, investigators have learned that the intruders apparently gained access to the databases through third-party applications on the Web site. "We have some ideas about what they are but we don't want to say until we finish the investigation," she said. Other databases at the law school, including those containing e-mail addresses or personal information about current students, employees and alumni, were unaffected by the incident, according to the school.
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9051420&taxonomyId=17&intsrc=kc_top

27. *December 05, Computerworld* – (National) **Privacy alert: Cookie variants can be used to skirt blockers, anti-spyware tools.** Just because your Web browser is set to block third-party tracking cookies, that doesn't mean all of them are being blocked. A growing number of Web sites are quietly resorting to the use of "first-party," subdomain cookies to skirt anti-spyware tools and cookie-blockers and allow third-party information-gathering and ad-serving, according to some privacy advocates and industry analysts. Though the cookies are not fundamentally different from other third-party cookies, they are very hard to detect and block, said a research engineer with CA's anti-

spyware research team. The result: companies could theoretically use the cookies to quietly gather and share consumer information with little risk of detection, he said. So far, the use of first-party, subdomain cookies appears to be less prevalent than standard third-party cookies, "but it's the kind of thing that might catch on quickly," he said. The growing, but largely hidden, issue of online consumer-tracking and information-sharing burst into the open in recent days because of the controversy generated by Facebook's Beacon ad-serving technology. First-party, subdomain cookies are those that appear to be served up by the primary Web site a user is visiting; in reality, they are being issued by an external third party. For example, a company whose primary domain name is xyz.com could create a subdomain called trackerxyz that falls within the xyz.com domain so it would look like this: www.trackerxyz.xyz.com. This subdomain actually points to a third party's server. But because the parent domain names are the same, the user's browser sees that server as belonging to the parent -- and treats cookies from both equally. In many cases, first-party, subdomain cookies serve legitimate purposes, said a marketing director at TRUSTe, a San Francisco-based online privacy certification organization. For instance, a bank might have a relationship with an external bill payment vendor, and it might set cookies that appear to come from the bank but actually have been set by the bill payment vendor.
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9051219&taxonomyId=17&intsrc=kc_top

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Communications Sector

28. *December 5, Associated Press* – (Northwest) **Officials: ham radio operators are storm's 'unsung heroes.'** When parts of Oregon were overwhelmed by wind and water during the recent storm, vital communication often was lacking, with trees down and across phone lines and cell coverage limited. Even the state police had difficulty in reaching some of their own troops. But ham radio worked. In fact, amateur radio operators were heralded by state emergency officials as heroes. Ham radio is more than just a hobby to some. It can set up networks for government and emergency officials to communicate when other communication services fail. "One of the problems in this is always communication," said Oregon's governor Tuesday. "I'm going to tell you who the heroes were from the very beginning of this...the ham radio operators. These people just came in and actually provided a tremendous communication link to us." A network of at least 60 volunteer amateur radio operators working along the coast and inland helped from keep crucial systems such as 911 calls, American Red Cross and hospital

services connected. They relayed information about patient care and relayed lists of supplies needed in areas cut off by water. In addition to getting an FCC license to operate, certain groups of operators are cleared by the federal government to work as emergency responders. The Oregon Office of Emergency Management said the radio operators were tireless in their efforts to keep the systems connected. It was ham radio that kept New York City agencies in touch with each other after their command center was destroyed on 9-11, according to the National Association for Amateur Radio. When hurricanes like Katrina hit, amateur radio helped provide life-and-death communication services when everything else failed.
Source: http://www.kptv.com/weatheralert/14776224/detail.html

29. *December 6, vnunet.com* – (National) **VoIP must connect to emergency services.** VoIP services that allow users to make calls to normal national phone numbers must also have the ability to connect to emergency numbers 999 and 112 from 8 September 2008. Ofcom wants to ensure that users who have switched to VoIP services from traditional landline or cellular phone companies can still access the relevant people in emergencies. The watchdog expressed concern that consumers needing to locate an ordinary landline or mobile phone in an emergency might face a delay of seconds or even minutes in getting through. "As new voice services develop and become more mainstream, regulation must evolve too," said the entity's chief executive. "Consumers must be confident that, if they can make calls to ordinary national numbers using their VoIP service, they will be able to call 999 or 112 in an emergency." Ofcom found that 78 per cent of VoIP users who cannot currently call 999 or 112 either believed that an emergency call was possible, or did not know whether or not this was the case. The ruling attempts to protect consumers amid increasing use of VoIP services and the trend to look and feel more like traditional fixed and mobile phone services. Some commentators have voiced concerns over a reliance on VoIP technology, following the Skype outage earlier this year.
Source: http://www.vnunet.com/vnunet/news/2205253/ofcom-voip-connect-emergency

[Return to top]

Commercial Facilities Sector

30. *December 5, ABC News* – (Nebraska; National) **Mall insecurity: Target for threats?** Police have long worried that malls are the perfect target for deranged criminals or terrorists. Recent mall shootings, including the deadly shooting in Omaha Wednesday, substantiate this concern. Last February, an 18-year-old fatally shot five people and injured four others during a mall shooting near Salt Lake City. In April, a mall shooting spree in Kansas City left three dead. And in 2002, the D.C. snipers murdered at least two people outside of strip malls. Last month, the FBI and Department of Homeland Security sent out a bulletin warning of a plot to target malls in major cities. The intelligence was determined to be of weak credibility, but underscores how seriously law enforcement deems the threat. Now the concern with the holiday season is that the latest tragedy in Omaha will spur copycats.
Source: http://abcnews.go.com/WN/LegalCenter/story?id=3960056

[Return to top]

National Monuments & Icons Sector

Nothing to report

[Return to top]

Dams Sector

31. *December 5, Herald-Citizen* – (Tennessee) **Public informed of Center Hill Dam progress.** For the first time since Center Hill Dam was deemed high risk by the U.S. Army Corps of Engineers in January, residents in Putnam County, Tennessee, were prepped on the project first hand at a public meeting held here last night. Both Corps officials and local emergency management agency directors were on hand for a brief presentation and to answer any questions residents had about the dam and its repairs, which are scheduled to begin in the next several weeks. The meeting last night was also one of the first times residents got to publicly view the flood inundation maps for the area. For Homeland Security reasons, the maps are currently only available at local Corps offices and at the offices of local county emergency management agencies. The project, which will cost $243 million to complete, is expected to be finished in 2013. Source: http://www.herald-citizen.com/NF/omf.wnm/herald/news_story.html?rkey=0047450+cr=gdn

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-5389
Subscription and Distribution Information:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-5389 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer